(12) UK Patent Application (19) GB (11) 2 404 263 (13) A

(43) Date of A Publication 26.01.2005

(21) Application No: 0415240.1

(22) Date of Filing: 07.07.2004

(30) Priority Data:
(31) 92118651 (32) 07.07.2003 (33) TW

(71) Applicant(s):
Yuen Foong Paper Co., Ltd
(Incorporated in Taiwan)
4F, 51, Sec 2, Chung Ching South Road,
Taipei, Taiwan

(72) Inventor(s):
Jia-Xin Zheng
Jia-Yan Lu
Jia-Feng Wu

(74) Agent and/or Address for Service:
Wilson Gunn M'Caw
5th Floor, Blackfriars House,
The Parsonage, MANCHESTER, M3 2JA,
United Kingdom

(51) INT CL[7]:
G06F 1/00

(52) UK CL (Edition X ):
G4A AAP A23D

(56) Documents Cited:
EP 1341071 A2 EP 1223495 A1
WO 1993/010509 A1

(58) Field of Search:
UK CL (Edition W ) G4A
INT CL[7] G06F
Other: WPI, EPODOC, PAJ, INSPEC, TXTE

(54) Abstract Title: **An access method for portable secure informaton**

(57) A portable secure information access system is disclosed. The system comprises a portable storage device 100 and a secure access module 111. The portable storage device comprises a disk partition 102, in which secure information is recorded, particularly in a concealed disk partition, and a secure computing module 103. The secure computing module 103 generates a session key (SK) in accordance with a challenge-response mechanism. The secure access module 111 receives the SK from the secure computing module, 103 encrypting or decrypting the secure information stored in the disk partition 102 in accordance with the SK so as to access the secure information.

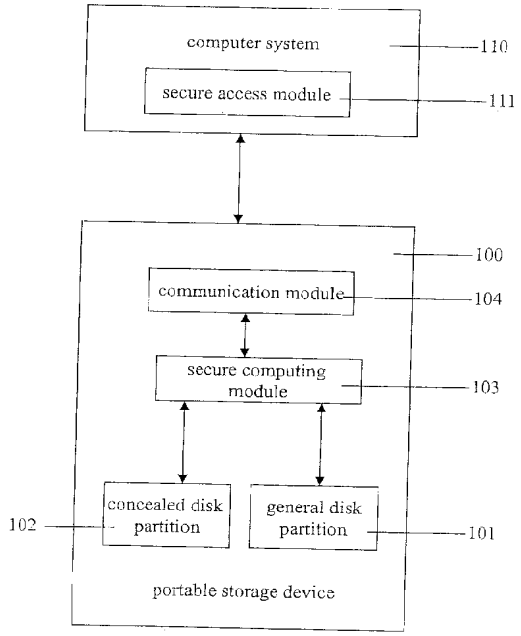


FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

Original Printed on Recycled Paper

GB 2 404 263 A

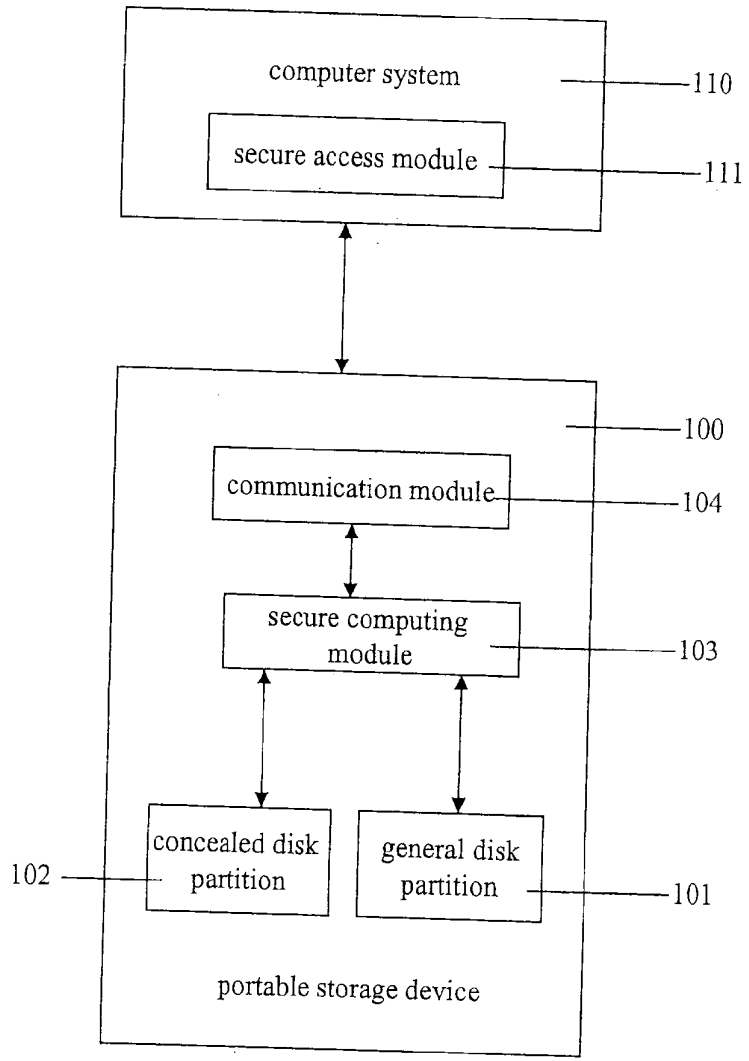
computer system
110
secure access module
111
100
communication module
104
secure computing module
103
concealed disk partition
102
general disk partition
101
portable storage device

FIG. 1

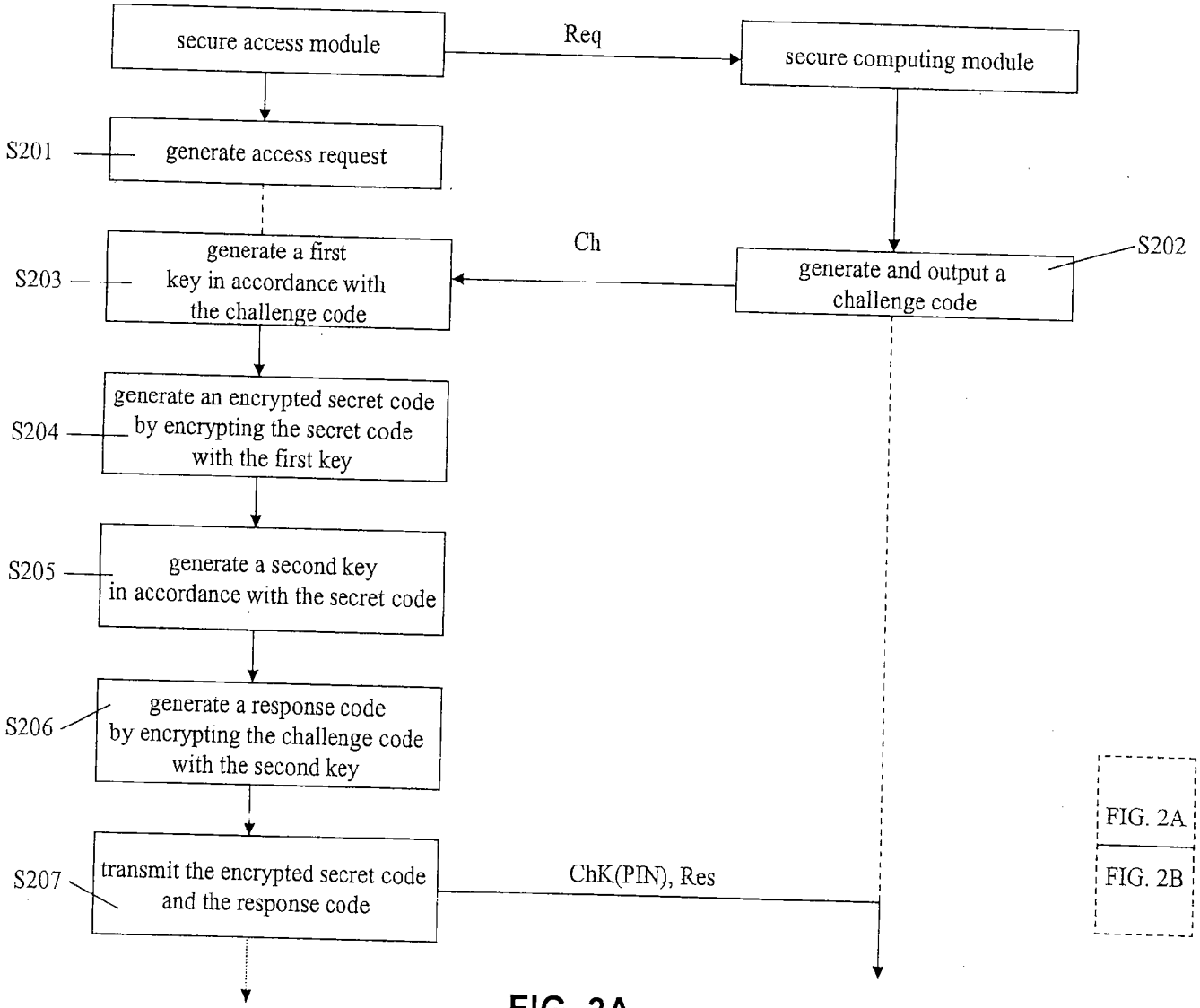


FIG. 2A



FIG. 2A
FIG. 2B

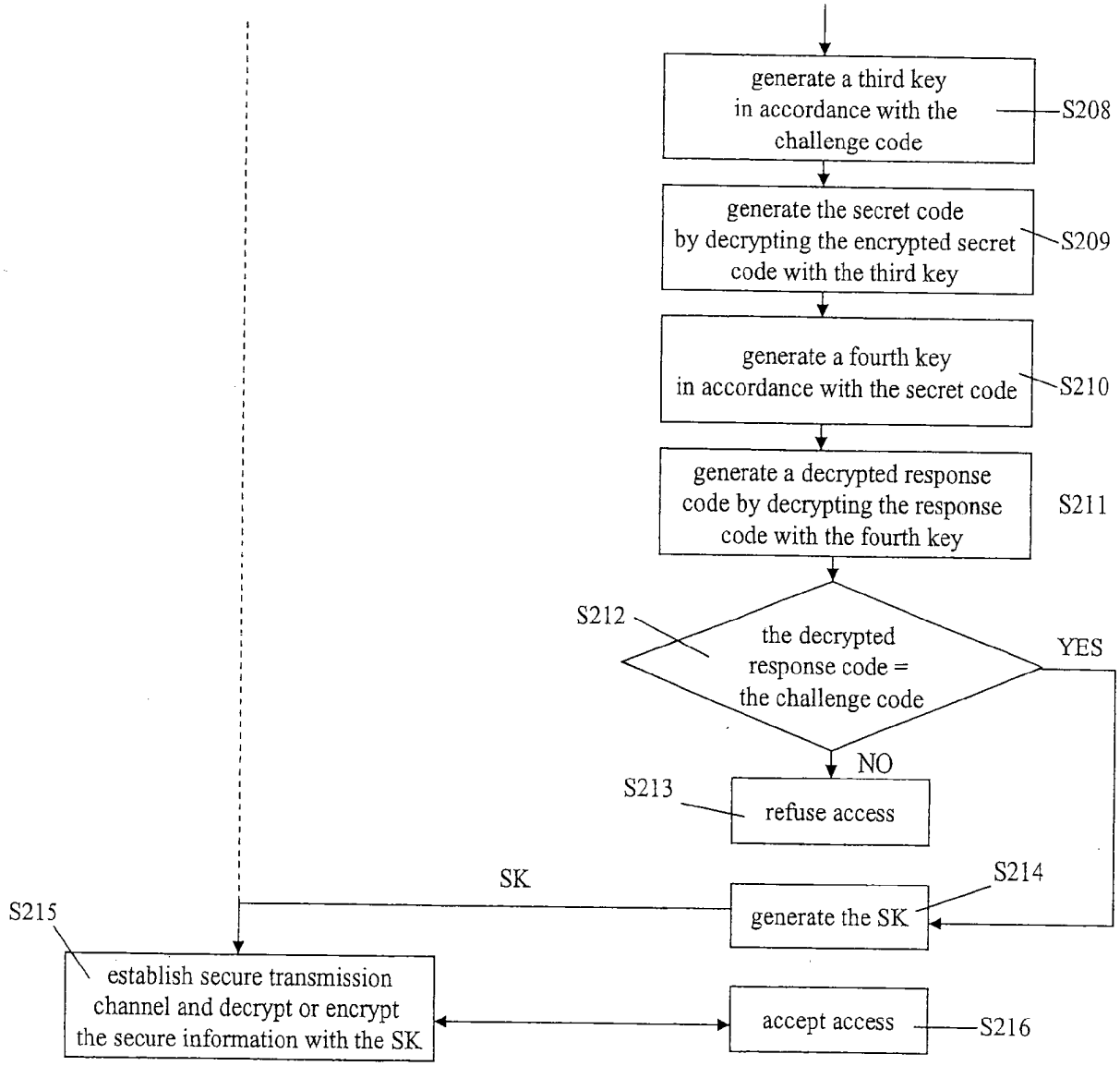
generate a third key in accordance with the challenge code
S208
generate the secret code by decrypting the encrypted secret code with the third key
S209
generate a fourth key in accordance with the secret code
S210
generate a decrypted response code by decrypting the response code with the fourth key
S211
S212
the decrypted response code = the challenge code
YES
NO
S213
refuse access
SK
S214
generate the SK
S215
establish secure transmission channel and decrypt or encrypt the secure information with the SK
accept access
S216

FIG. 2B

# PORTABLE SECURE INFORMATION ACCESS SYSTEM, PORTABLE STORAGE DEVICE AND ACCESS METHOD FOR PORTABLE SECURE INFORMATION

## FIELD OF THE INVENTION

[0001] The present invention relates to a secure information access system and method; and more particularly to a portable secure information access system, a portable storage device and an access method for portable secure information

## BACKGROUND

[0002] The human lifestyle is already facing major changes as a consequence of the popularization of computers and networks. For example, the establishment and management of digital data has already replaced the traditional modes of paper usage, the Internet has already become the best method for people to collect data, and people are performing commercial exchanges using the Internet, such as shopping and investing in stocks, etc. In contrast, due to the influence of information and digitization of human life, related problems concerning network security, protection of privacy of personal data, and authentication of identity, etc., have already become serious problems which require priority solutions.

[0003] The problems of network security, protection of privacy of personal data, and authentication of identity can be solved by utilizing secure information, such as keys and personal private data. For example, Internet service providers, before providing network services, can perform authentication of identity by examining personal private data in order to confirm whether or not the operators are legitimate users, or when receiving data they can perform identification of the user's key in accordance with related public-key cryptography technology in order to confirm the user's identity.

[0004] However, no effective management mechanism exists for the above-described personal secure information, and the well-known management scheme is for the user to voluntarily store the secure information on the related storage medium, such as a magnetic disk, in order to avoid the possibility that the secure information may be deleted or stolen when other users use the same computer. However, because magnetic disk space is limited, one cannot store a large quantity of private information. Also there is no way to increase the use value. In addition, because there has not yet been established any related mechanism that can protect

secure information on a storage medium, other than simply being able to control whether or not one can provide a computer system to access the secure information by means of a switch, in the event that the user loses the storage medium, there still is an opportunity for the secure information on the storage medium to be stolen.

## SUMMARY OF THE INVENTION

[0005] A portable secure information access system is disclosed. The system comprises a portable storage device and a secure access module. The portable storage device comprises a disk partition in which to record a secure information and a secure computing module. The secure access module receives a session key (SK) from the secure computing module, encrypting or decrypting the secure information stored in the disk partition in accordance with the SK so as to access the secure information.

[0006] A portable storage device comprises a disk partition and a secure computing module. The disk partition records a secure information. The secure computing module generates a session key (SK) in accordance with a challenge-response mechanism.

[0007] An access method for portable secure information is disclosed. The access method comprises: generating a session key (SK) in accordance with a challenge-response mechanism; and encrypting and decrypting a secure information in accordance with the SK.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Fig. 1 is a schematic drawing showing an exemplary portable secure information access system.

[0009] FIGS. 2A and 2B are an operational flow showing an exemplary access method for secure information.

## DETAILED DESCRIPTION

[0010] This description of the exemplary embodiments is intended to be read in connection with the accompanying drawings, which are to be considered part of the entire written description. In the description, relative terms such as "lower," "upper," "horizontal," "vertical,", "above," "below," "up," "down," "top" and "bottom" as well as derivative thereof (e.g., "horizontally," "downwardly," "upwardly," etc.) should be construed to refer to the orientation as then described or as shown in the drawing under discussion. These relative terms

are for convenience of description and do not require that the apparatus be constructed or operated in a particular orientation. Terms concerning attachments, coupling and the like, such as "connected" and "interconnected," refer to a relationship wherein structures are secured or attached to one another either directly or indirectly through intervening structures, as well as both movable or rigid attachments or relationships, unless expressly described otherwise.

[0011] FIG. 1 is a schematic drawing showing an exemplary portable secure information access system.

[0012] The portable secure information access system according to this embodiment comprises a portable storage device 100 and a computer system 110 having a secure access module 111. The present invention can be embodied on any form of portable storage medium, such as mobile hard disk or flash memory, or the like.

[0013] The portable storage device 100 includes a general disk partition 101, a concealed (first) disk partition 102, a secure computing module 103, and a communication module 104. In the general disk partition 101, general insecure data can be stored therein. In the concealed disk partition 102, related secure information, such as personal secret keys, certificate files, and personal private data, etc., can be stored. In this embodiment for security considerations the disk partition 102 is designed to be concealed, that the concealed disk partition 102 and the secure information therein cannot be detected and examined by the operating system of the computer system 110, and that there is no way to perform access using general file management tools in the computer system 110. Alternatively, the disk partition 102 can be designed as not concealed, but, the secure information in the disk partition 102 must be accessed by means of the mechanism of the present invention in order to achieve the purpose of secure access. Under actually made examples, the concealed disk partition 102 can be specified as 16K-256K or higher. Other than this, the data stored in the general disk partition 101 can be directly accessed by means of the operating system or file management tools in the computer system 110.

[0014] The secure computing module 103 can be established in firmware in the portable storage device 100, and it is mainly responsible for computation required for communication with the secure access module 111 in the computer system 110. The communication module 104 is responsible for processing required for communication between the portable storage device 100 and the computer system 110. In some embodiments, the portable storage device 100 can be connected with the computer system 110 by means of a universal serial bus (USB), at which

time, the communication module 104 then is responsible for related processing of USB interface communication between the portable storage device 100 and the computer system 110.

[0015] The secure access module 111 in the computer system 110 is designed to access secure information in the concealed disk partition 102 and data in the general disk partition 101. In addition, the secure access module 111 also can ensure information security during data transmission between the portable storage device 100 and the computer system 110. The secure access module 111 can obtain a session key (SK) from the secure computing module 103 in accordance with a security mechanism such as a challenge-response mechanism, and furthermore perform encryption and decryption of the secure information in the concealed disk partition 102 in accordance with the session key, in order to securely access the secure information. The challenge-response mechanism can be, for example, a hand-shaking mechanism. The secure transmission mechanism between the secure computing module 103 and the secure access module 111 is explained below.

[0016] FIGS. 2A and 2B are an operational flow chart diagram showing an exemplary access method for secure information.

[0017] First, as in step S201, the secure access module 111 generates an access request Req, and furthermore transmits the access request Req to the secure computing module 103. After that, as in step S202, the secure computing module 103 in response to the access request Req generates an access right code hd and in addition generates a challenge code Ch, and furthermore transmits the challenge code Ch to the secure access module 111. In connection with the access request made by the secure access module 111 at this time, all of the information exchanges between the secure access module 111 and the secure computing module 103 may include this access right code hd and perform identification in accordance with this access right code hd.

[0018] Next, as in step S203, the secure access module 111 derives a first key ChK in accordance with the challenge code Ch and a prescribed algorithm, and furthermore as in step S204, uses the first key ChK to perform encryption of a secret code PIN in response to the challenge code Ch, whereby to generate an encrypted secret code ChK(PIN). The prescribed algorithm can be a scheme which converts a prescribed character string into a Triple DES encryption key in accordance with the Password-Based Cryptography Standard (PBCS) of the Public-Key Cryptography Standards (PKCS) (PKCS #5).

[0019] After that, as in step S205, the secure access module 111 derives a second key PK in accordance with the secret code PIN and the prescribed algorithm, and furthermore as in step S206, uses the second key PK to perform encryption of the challenge code Ch, whereby to generate a response code Res. After that, as in step S207, the secure access module 111 transmits the encrypted secret code ChK(PIN) and the response code Res to the secure computing module 103.

[0020] Next, as in step S208, the secure computing module 103 derives a third key ChK' in accordance with the challenge code Ch and the prescribed algorithm, and furthermore as in step S209, uses the third key ChK' to perform decryption of the encrypted secret code ChK(PIN), whereby to obtain the secret code PIN. After that, as in step S210, the secure computing module 103 derives a fourth key PK' in accordance with the secret code PIN and the prescribed algorithm, and furthermore as in step S211, uses the fourth key PK' to perform decryption of the response code Res, thereby to obtain a decrypted response code Res'.

[0021] After that, as in step S212, the secure computing module 103 determines whether or not the decrypted response code Res' is identical to the challenge code Ch, and if the decrypted response code Res' is different from the challenge code Ch (No in step S212), then as in step S213, the secure computing module 103 refuses access activity of the secure access module 111. But if the decrypted response code Res' is identical to the challenge code Ch (Yes in step S212), then as in step S214, the secure computing module 103 uses a random number scheme to generate a session key SK, and furthermore transmits the session key SK to the secure access module 111.

[0022] In some embodiments, the first, second, third and fourth keys can be, for example, symmetric keys.

[0023] After the secure access module 111 receives the session key SK, as in step S215, it then can establish a secure transmission channel with the secure computing module 103, and furthermore it can perform encryption and decryption of secure information transmitted between the secure access module 111 and the secure computing module 103 in accordance with the session key SK, in order to securely access the secure information in the concealed disk partition 102. At this time, the secure computing module 103 can, as in step S216, accept access activity of the secure access module 111. However, after the conclusion of this time of access by the secure access module 111, the secure computing module 103 can set the session key SK to

NULL in order to nullify the secure transmission channel between the secure access module 111 and the secure computing module 103.

[0024] As stated above, the secure access module 111 also can ensure information security during data transmission between the portable storage device 100 and the computer system 110. Therefore, before the secure computing module 103 transmits the session key SK to the secure access module 111, the secure computing module 103 can derive a fifth key ResK in accordance with the response code Res and the prescribed algorithm, and furthermore use the fifth key ResK to perform encryption of the session key SK, thereby to generate an encrypted session key ResK(SK), and furthermore transmit the encrypted session key ResK(SK) to the secure access module 111. After the secure access module 111 receives the encrypted session key ResK(SK), the secure access module 111 derives the fifth key ResK in accordance with the response code Res and the prescribed algorithm, and performs decryption of the encrypted session key ResK(SK) in accordance with the fifth key ResK, whereby to obtain the session key SK.

[0025] In another aspect, in order to convert secure information such as personal secret keys so as to conform to various international key storage token interface standards, one can establish a conversion element (not illustrated in the drawing) in the computer system and use it to perform conversion of secure information acquired from the portable storage device 100 such that the secure information after conversion conforms to international cryptographic token interface standards, such as Cryptographic Service Provider (CSP) led by Microsoft, Cryptographic Token Interface Standard (CTIS) of the Public-Key Cryptography Standards (PKCS) (PKCS #11) led by RSA Laboratories, and Cryptographic Service Provider (CSP) meeting JAVA standard. Of these, the conversion element at least provides functions such as session/thread management, key generation/management, key exchange, data encryption/decryption, hash function, and signature generation/verification.

[0026] Therefore, by a portable secure information access system and method based on the present invention, one can securely access secure information in a portable storage medium by means of an effective mechanism. At the same time, if the portable storage medium is lost, the secure information in the concealed disk partition will receive protection and will not end up being stolen.

[0027] Although the invention has been described in terms of exemplary embodiments, it is not limited thereto. Rather, the appended claims should be construed broadly, to include other variants and embodiments of the invention, which may be made by those skilled in the art without departing from the scope and range of equivalents of the invention.

## CLAIMS

1. A portable secure information access system, comprising:

a portable storage device comprising:

a disk partition in which a secure information is recorded; and

a secure computing module; and

a secure access module receiving a session key (SK) from the secure computing module, for encrypting or decrypting the secure information stored in the disk partition in accordance with the SK so as to access the secure information.

2. The portable secure information access system of claim 1, wherein the secure access module receives the SK from the secure computing module in accordance with a challenge-response mechanism.

3. The portable secure information access system of claim 2, wherein the challenge-response mechanism comprises a hand-shaking mechanism.

4. The portable secure information access system of claim 2, wherein, before generating the SK, the secure access module outputs an access request to the secure computing module so as to generate a challenge code; the secure computing module transmits the challenge code to the secure access module; the secure access module outputs an encrypted secret code and a response code which are generated in accordance with the challenge code to the secure computing module; the secure computing module decrypts the encrypted secret code and the response code so as to generate a decrypted response code; and the secure computing module compares the challenge code with the decrypted response code so as to determine whether to generate the SK.

5. The portable secure information access system of claim 4, wherein, before outputting the encrypted secret code and the response code, the secure access module generates a first key in accordance with the challenge code and a prescribed algorithm; generates the encrypted secret code by encrypting a secret code with the first key; generates a second key in accordance with the secret code and the prescribed algorithm; and generates the response code by encrypting the challenge code with the second key.

6. The portable secure information access system of claim 4, wherein, before generating the decrypted response code, the secure computing module generates a first key in accordance with the challenge code and a prescribed algorithm; generates a secret code by decrypting the encrypted secret code with the first key; generates a second key in accordance the secret code and the prescribed algorithm; and decrypts the response code with the second key..

7. The portable secure information access system of claim 2, wherein, before receiving the SK, the secure access module outputs an access request to the secure computing module so as to generate a challenge code; the secure computing module transmits the challenge code to the secure access module; the secure access module generates a first key in accordance with the challenge code and a prescribed algorithm, generates the encrypted secret code by encrypting an secret code with the first key, generates a second key in accordance wit the secret code and the prescribed algorithm, generates the response code by encrypting the challenge code with the second key, and outputs the encrypted secret code and the response code to the secure computing module; the secure computing module generates a third key in accordance with the challenge code and the prescribed algorithm, generates the secret code by decrypting the encrypted secret code with the third key, generates a fourth key in accordance the secret code and the prescribed algorithm, and generates a decrypted response code by decrypting the response code with the fourth key; and the secure computing module compares the challenge code with the decrypted response code so as to determine whether to generate the SK.

8. The portable secure information access system of claim 4, wherein, before generating the SK, the secure computing module further generates a key in accordance with the response code; encrypts the SK with the key so as to generate an encrypted SK; and transmits the encrypted SK to the secure access module, and the secure access module generates an additional key in accordance with the response code; and decrypts the encrypted SK with the additional key.

9. The portable secure information access system of claim 7, wherein, before generating the SK, the secure computing module further generates a key in accordance with the response code; encrypts the SK with the key so as to generate an encrypted SK; and transmits the encrypted SK to the secure access module, and the secure access module generates an additional key in accordance with the response code; and decrypts the encrypted SK with the additional key.

10. The portable secure information access system of claim 9, wherein the key is substantially similar to the additional key.

11. The portable secure information access system of claim 2, wherein the secure computing module nullifies the SK in response to a conclusion of access of the secure information.

12. The portable secure information access system of claim 4, wherein the secure computing module generates the challenge code using a random number scheme.

13. The portable secure information access system of claim 4, the secure computing module generates the SK using a random number scheme.

14. The portable secure information access system of claim 5 or 6, wherein the prescribed algorithm converts a prescribed character string into a Triple DES encryption key in accordance with Password-Based Cryptography Standard (PBCS) of Public-Key Cryptography Standards (PKCS).

15. The portable secure information access system of any preceding claim, further comprising a conversion module converting the secure information into a converted secure information, the converted secure information satisfying an international cryptographic token interface standard.

16. The portable secure information access system of any preceding claim, wherein the disk partition is not detected by an operating system of a computer system and the secure information therein is not accessible by using a file management tool in the computer system.

17. An access method for portable secure information, comprising:
generating a session key (SK) in accordance with a challenge-response mechanism; and
encrypting and decrypting a secure information in accordance with the SK.

18. The access method for portable secure information of claim 17, wherein the challenge-response mechanism comprises a hand-shaking mechanism.

19. The access method for portable secure information of claim 17, wherein the step of generating the SK comprises:

outputting an access request so as to generate a challenge code;

outputting an encrypted secret code and a response code generated in accordance with the challenge code;

decrypting the encrypted secret code and the response code so as to generate a decrypted response code; and

comparing the challenge code with the decrypted response code so as to determine whether to generate the SK.

20. The access method for portable secure information of claim 19, wherein the step of outputting the encrypted secret code and the response code comprises:

generating a first key in accordance with the challenge code and a prescribed algorithm;

generating the encrypted secret code by encrypting a secret code with the first key;

generating a second key in accordance with the secret code and the prescribed algorithm;

generating the response code by encrypting the challenge code with the second key; and

outputting the encrypted secret code and the response code.

21. The access method for portable secure information of claim 19, wherein the step of decrypting the encrypted secret code and the response code so as to generate a decrypted response code comprises:

generating a first key in accordance with the challenge code and a prescribed algorithm;

generating a secret code by decrypting the encrypted secret code with the first key;

generating a second key in accordance with the secret code and the prescribed algorithm; and

generating the decrypted response code by decrypting the response code with the second key.

22. The access method for portable secure information of claim 17, wherein the step of generating the SK comprises:

outputting an access request so as to generate and output a challenge code;

generating a first key in accordance with the challenge code and a prescribed algorithm;

generating the encrypted secret code by encrypting a secret code with the first key;

generating a second key in accordance with the secret code and the prescribed algorithm;

generating the response code by encrypting the challenge code with the second key;

outputting the encrypted secret code and the response code;

generating a third key in accordance with the challenge code and the prescribed algorithm;

generating a secret code by decrypting the encrypted secret code with the third key;

generating a fourth key in accordance the secret code and prescribed algorithm;

generating the decrypted response code by decrypting the response code with the fourth key; and

comparing the challenge code with the decrypted response code so as to determine whether to generate the SK.

23. The access method for portable secure information of claim 19, wherein the method of generating the SK further comprises:

generating an key in accordance with the response code;

encrypting the SK with the key so as to generate an encrypted SK;

transmitting the encrypted SK;

generating an additional key in accordance with the response code; and

decrypting the encrypted SK with the additional key.

24. The access method for portable secure information of claim 18, wherein the key is substantially equivalent to the additional key.

25. The access method for portable secure information of claim 17, further comprising nullifying the SK in response with a conclusion of access of the secure information.

26. The access method for portable secure information of claim 19, wherein the step of generating the challenge code uses a random number scheme.

27. The access method for portable secure information of claim 19, the step of generating the SK uses a random number scheme.

28. The access method for portable secure information of claim 22, wherein the step of generating the challenge code uses a random number scheme.

29. The access method for portable secure information of claim 22, the step of generating the SK uses a random number scheme.

30. The access method for portable secure information of claim 20 or 21, further comprising converting a prescribed character string into a Triple DES encryption key in accordance with Password-Based Cryptography Standard (PBCS) of Public-Key Cryptography Standards (PKCS).

31. The access method for portable secure information of claim 17, further comprising converting the secure information into a converted secure information, the converted secure information satisfying an international cryptographic token interface standard.

32. A portable storage device, comprising:

a disk partition in which a secure information is recorded; and

a secure computing module, the secure computing module generating a session key (SK) in accordance with a challenge-response mechanism.

33. The portable storage device of claim 32, wherein the challenge-response mechanism comprises a hand-shaking mechanism.

34. The portable storage device of claim 32, wherein the secure computing module generates a challenge code in accordance with an access request; outputs the challenge code; receives an encrypted secret code and a response code which are generated in accordance with the challenge code from the secure computing module; decrypts the encrypted secret code and the response code so as to generate a decrypted response code; and compares the challenge code with the decrypted response code so as to determine whether to generate the SK.

35. The portable storage device of claim 34, wherein, before generating the decrypted response code, the secure computing module generates a first key in accordance with the

challenge code and a prescribed algorithm; generates a secret code by decrypting the encrypted secret code with the first key; and generates a second key in accordance the secret code and the prescribed algorithm; and decrypting the response code with the second key.

36. The portable storage device claim 34, wherein, before generating the SK, the secure computing module further generates an key in accordance with the response code; encrypts the SK with the key so as to generate an encrypted SK; and outputs the encrypted SK.

37. The portable storage device of claim 32, wherein the secure computing module nullifies the SK in response to a conclusion of access of the secure information.

38. The portable storage device of claim 34, wherein the secure computing module generates the challenge code using a random number scheme.

39. The portable storage device of claim 34, wherein the secure computing module generates the SK using a random number scheme.

40. The portable storage device of claim 31, wherein the prescribed algorithm converts a prescribed character string into a Triple DES encryption key in accordance with Password-Based Cryptography Standard (PBCS) of Public-Key Cryptography Standards (PKCS).

41. The portable storage device of claim 32, further comprising a conversion module for converting the secure information into a converted secure information, the converted secure information satisfying an international cryptographic token interface standard.

42. The portable storage device of claim 32, wherein the disk partition is not detected by an operating system of a computer system and the secure information therein is not accessible by using a file management tool in the computer system.

43. The portable secure information system as claimed in any of claims 5 to 10 wherein the or each key is a symmetric key.

44. The access method for portable secure information of any of claims 20 to 24 wherein the or each key is a symmetric key.

45. The portable storage device of claim 35 or 36 wherein the or each key is a symmetric key.

46. A portable secure information access system substantially as herein described with reference to the accompanying drawings.

47. An access method for portable secure information substantially as herein described with reference to the accompanying drawings.

48. A portable storage device substantially as herein described with reference to the accompanying drawings.

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office
INVESTOR IN PEOPLE

**Application No:** GB0415240.1 **Examiner:** Mr Adam Tucker

**Claims searched:** 1-48 **Date of search:** 18 November 2004

# Patents Act 1977: Search Report under Section 17

**Documents considered to be relevant:**

| Category | Relevant to claims | Identity of document and passage or figure of particular relevance |
|---|---|---|
| X,P | 32 | EP1341071 A2 (Matsushita) See whole document |
| X | 32, 33 & 37 | EP1223495 A1 (Hewlett-Packard) See in particular paras 9-13 & 28-30 |
| X | 17, 18 & 25 | WO93/10509 A1 (Security Domain) See in particular the abstract, page 2 lines 5-30, page 8 line 25-page 9 line 15 and page 11 lines 29-32 |

Categories:

| | | | |
|---|---|---|---|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art. |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category. | P | Document published on or after the declared priority date but before the filing date of this invention. |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |

**Field of Search:**

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC$^{W}$ :

G4A

Worldwide search of patent documents classified in the following areas of the IPC$^{07}$

G06F

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, PAJ, INSPEC, TXTE